-STUDY GUIDE-

Y-MUN TRAINING DEVELOPMENT CONFERENCE

SPECPOL

TABLE OF CONTENTS

I. Letter by the Secretary-General

Esteemed delegates of SPECPOL,

It is with great pleasure that I welcome you all to the 10th edition of Yeditepe Model United Nations Training and Development Conference as the Secretary-General. Organized by the oldest Model United Nations Club in Turkey, every year we try to use our knowledge to provide our participants with an exceptional MUN experience.

Being aware of the current issues that our world is facing, Y-MUN 2017 will simulate 16 different committees. Most of the committees aim to give our participants a demonstration of the world's most urgent problems while some special committees will take you to the past to simulate some crucial events. With our brilliant Academic Team, we are working to provide you the finest academic experience.

In SPECPOL the delegates will tackle the issue which get more important every day which is cybersecurity. I would like to thank Ms. Nilsu Can for her efforts in creating this committee. Lastly, I would like to give my thanks to my Deputy Secretary-General Mr. Uygar Berk Edebali who supported me greatly during this process and also Mr. Onuralp Acar and his deputies Ms. Dilruba Akçınar and Mr. Ömer Cem Sipahi for their work in creating this amazing conference.

Welcome where the journey begins!

Ege SÜREK
Secretary-General of Y-MUN 2017

II. Letter by Under Secretary-General

Distinguished Delegates,

With my utmost pleasure, I would like to welcome you to the committee Special Political, Decolonization of Yeditepe University Model United Nations Training, and Development Conference Y-MUN 2017. My name is Nilsu Can, and I am a third-year student at Istanbul Bilgi University, Business Administration Faculty. I have been participating in Model United Nations conferences since 2015, and Y-MUN 2015 was my very first conference in my Model United Nations career.

This year's conference confronts the serious challenges facing the international community. I hope that you are as passionate as I am for an incredible three days of debate, diplomacy, and international exchange.

I hope that this topic can create an enjoyable debate that each participant can join and enjoy. This study guide had been prepared to give background and general knowledge about the topic. Delegates expected to fulfill their knowledge with their further researches. At Y-MUN, you will consider inventive solutions to earnest global problems. Many diplomats have contemplated the same issues and, as of yet, still, struggle to settle key questions over responsibility and sovereignty. The delegates at this conference will have the chance to debate critical topics while learning various perspectives on them.

Last but not least, I would like to thank honorable Secretary General Ms. Ege Sürek for her kindness, understanding and also for her efforts, and dear Deputy Secretary-General Mr. Onuralp Acar for his energy, at most thank both of you for giving me a chance to be an Under-Secretary-General of Y-MUN 2017.

Please do not hesitate to say hello or to ask any questions; consider me, as well as the rest of our staff, at your service. With that, welcome to Y-MUN 2017!

Sincerely

Nilsu Can

Under Secretary-General of SPECPOL

III. Introduction to Topic

Outage of network, hacking, computer viruses and incidents like these affects companies or even governments as the usage of internet, data networks, and digital platforms increase

When we check the history the ‘’net’’ has been around for over 50 years. During the Cold War in the United States, there was a university experiment in military communications. The idea was to connect many computers to a network instead of in a straight line. On the other hand, technological advances presented by the Soviet Union during the Cold War were required as a serious threat by the American government: The possibility of a nuclear attack. Pentagon thought if there was a nuclear attack on the United States, there is a little possibility that the entire network would be damaged, so they could still send and receive intelligence. In this sense, in 1957 the American government created an organization, the Advanced Research Projects Agency (ARPA), with the primary objective of developing research projects on computing technology.

In the beginning, the computers were attached by cables. With the developing connection and network systems, they utilized telephone system on mentioned technology and decreased the physical attachments. Once people realized that they could communicate with other people by using this computer network, they began to demand access. First users were from the university and government sectors. However, much more people started to get access to computer networks. With that, many community groups established networks that different from the official networks to use in their communities. After expanding networks, connections and developing technologies the ‘’internet’’ has shaped as if today. A military action has become a fundamental of communication and technology.

William Gibson first used the word of "Cyberspace" in his fantasy novel Neuromancer, to describe the "world" of computers, and the society that gathers around them. His imaginary world became real in these days.

In recent years, cyberspace has emerged as the critical differentiator for economic and social progress. Cyberspace is providing opportunities to individuals, governments, small businesses and large companies to shape their goals, with over 3.5 billion internet users in the world. The cyberspace also offers an environment for innovations, which creates opportunities potentially disrupting businesses, governance, and our daily lives.

In a quite short time, people and companies have attached cyberspace to create new industries, social area and a new economic circle that has and affects our lives. Meantime, individuals, different national groups, and governments are using cyberspace for their harmful interests. Terrorists threaten, track and target through the Internet, hackers steal data, and intelligence services deportment intelligence. However, most of the majority of cyberspace is civilian space used by individuals, businesses, and governments for legal purposes. There are a respectable amount of breaches through the cybersecurity. Governments, special agencies, and organizations spent the effort to protect the cybersecurity, confidentiality of individuals and governments. They also gather to build the Law of Cyber-Space to ensure mentioned before.

IV. Definitions

Cyber: A combining form meaning “computer”, “computer network”, or “virtual reality”, used in the formation of compound words.

Terrorism: The unlawful use of violence and intimidation, especially against civilians, in the pursuit of political aims.

Cyber-warfare: The use of computer technology to disrupt the activities of a state or organization, especially the deliberate attacking of information systems for strategic or military purposes.

Cyber Security: Cybersecurity refers to the measures taken to keep electronic information private and safe from damage or theft. It is also used to make sure these devices and data are not misused. Cybersecurity applies to both software and hardware, as well as information on the Internet, and can be used to protect everything from personal information to complex government systems.

Intranets: An intranet is a private network that can only be accessed by authorized users. The prefix "intra" means "internal" and therefore implies an intranet is designed for internal communications.

Malware: Is a malicious software, a program or a file that is harmful to a computer user. Malware includes computer viruses, worms, Trojan horses, and spyware.

DoS Attack: Denial of service attack is a network or system traffic to overwhelm the abused resources, and it aimed at preventing a machine or network resources from being accessed by actual users.

Virus: A type of malicious code or program written to alter the way a computer operates and that is designed to spread from one computer to another. A virus operates by inserting or attaching itself to a legitimate program or document that supports macros to execute its code.

Cyber ethics: Cyber ethics is the philosophic study of ethics about computers, encompassing user behavior and what computers are programmed to do, and how this affects individuals and society. For years, various governments have enacted regulations while organizations have defined policies about cyber ethics.

ICT: Information and communications technology(ICT) refers to all the technology used to handle telecommunications, broadcast media, intelligent building management systems, audiovisual processing, and transmission systems, and network-based control and monitoring functions. Although ICT often considered an extended synonym for information technology (IT), its scope is broader.

V. Threats, Challenges & Opportunities for Cyber Security

Cyber security and cyber breaches today is the biggest fear for critic and complex infrastructure like telecommunications, banking, power, etc. These recent worldwide devastating attacks that proved the dark side of digitalization.

Cyber-attacks are damaging to businesses and government agencies and threaten millions of personal data of users

One of the biggest challenges in cyberspace acquires from the combinations of impacts which refers capability evolution in information technology, the interconnectivity it enables, and the following ability of states and non-state organizations and actors to do both harm and good. The extensive interconnected and complex structure of cyberspace makes it difficult to determine the interests of governments, problems and the strategy for issues like attribution, recovery, and reconstitution of systems after an occasion. The risk perspective contains both technical and non-technical dangers. Technical dangers can considerably harm government systems and critical infrastructure, the confidentiality and integrity of government and private sector data, and individual identity, information.

VI. The Difference between Cyber-Terrorism and Cyber-Crime

The difference between cyber-terrorism and cyber-crime is the "impulse." The same action could be taken by a cyber-terrorist and a cyber-criminal (i.e. hacking an account to steal the

information.) Still the difference is "why?". A terrorist group, such as Anonymous, let everyone know what that they did, they inform you. But a criminal sneak into information and do not want it to be found out that what they did.

V. Cyber-Terrorism in a Framework

Today, information technologies, systems are the fundamentals of the globalization and have a great importance in our everyday lives such as communication, energy, transportation, electrical, water, and banking. With the rise and usage of technology, these systems become vulnerable and open to cyber-attacks.

While usage of internet increases and becoming more dependent on technology, usage areas of mobile phones through cities, so the cyber-threats increase.

As a whole, cyberterrorism wasn’t popular until the end of the millennium. There were many crazy scenarios which apparently did not be revealed. Nevertheless, the fear of what might happen, either on purpose or by accident, if computers or technology were to go wrong, continued.

"Cyber-Terrorism" has no one specific definition but term includes acts of internet vandalism, "hacktivism" or cybercrime which these acts don't directly threaten lives or livelihoods of their victims. Cyber terrorists perform with the focusing on damaging and destruction of their activities.

In contrast to conventional terrorism, cyber terrorism applies harmful computer technology instead of physical force. However, cyber terrorism uses political, religious or ideological goals to harm civilians by physically or psychologically. There against while cyber-terrorists use malware and viruses to disable the military targets, cyber-criminals harms individuals by

bullying or revenging despite the political or economic goals. Sometimes these differentiation conflicts and it gets hard to separate.

National states may act like cyber-terrorist to steal money, identities or data, or act like hacktivists. It is about the actors' intention and identity, and there are not usually known.

VI. Past Cyber Attacks and Following Actions

The very first cyber-attack recorded in 1998 from a Sri Lankan guerillas ‘’Black Tigers’’. They have written special software to jam Sri Lanka's ambassadors' email inboxes with hundreds of emails, for a couple of weeks. The same year, during the Kosovo War, NATO computers were exposed to DoS attacks and e-mail bombs. This breakdown was against US government websites, and the attack was directed by Chinese activists, which was an act of revenge to NATO forces for bombing accidentally Chinese embassy in Belgrade.

a. ESTONIA

In 2007 government of Estonia decided to move Bronze Soldier from Tallinn to a military cemetery, out of the city because for the Estonians sculpture is a painful symbol of Soviet abuse. On 27 April, Estonia was exposed to a cyber-attack, in some situations it lasted weeks. Media organs, online government organs, and banks were slowed never seen before. Almost every online organ, servers were failed by huge amounts of online requests and botnets. Communication by email was unable, and ATM's were emptied out by Estonians, there were no cash flows in the banks and newspapers couldn’t deliver the news.

Attacks came from Russian IP addresses, and the online instructions were in Russian, but due to Article 5, NATO members could defend each other only if a cyber-attack results in a major

loss of life equivalent to military action. Therefore, identifying who is responsible was impossible, and Estonia's requests for help to Moscow were ignored.

b. UNITED STATES OF AMERICA

In 2008 there was a cyber-attack on the United States which named was "the worst breach of U.S. military computers in history". This attack caused to the establishment of U.S. Cyber Command. It started a USB flash drive was left in the Department of Defense facility base in the Middle East, in a parking lot, and USB flash drive infected by a foreign intelligence agency and the transmission of the virus completed through a laptop that belongs U.S. Central Command. Pentagon almost worked for one and a half year to clean the virus from the military network system. The virus, "agent.btz", defined by the authorities as "can scan computers for data, open backdoors, and send through those backdoors to a remote command and control server" which was a major threat for the U.S. and they suspected from Russian hackers. After this situation, Pentagon banned USB drives.

c. CHINA

Between September 2012 and March 2013, the Chinese media has released that 85 public institutions' and companies' websites were hacked and 39 of the attacks were coming from American IP addresses. At the same time, China has reported that there had been 5800 hacking attempts from the United States. IP addresses. These IP addresses contained 73 percent of the information that had been stolen in attacks against Chinese customers.

Western countries have accused China for a long time of spying but officials and organizations have followed the attacks on corporate infrastructure and the computer systems in their countries to China. China has denied the accusation by saying "It is nearly impossible to know whether or not an attack is government-sponsored because of the difficulty in tracking true identities in cyberspace".

d. FRANCE

In December 2010, just before the Paris G20 Summit, there was a cyber-attack against G20 Summit. It all began an e-mail sent to the French Ministry of Finance. The e-mail's attachments were a "trojan horse" type virus in a malware-based PDF document. When the document was opened, the virus had spread through the other governmental computers and continued to spread as forwarded e-mails to the other officials. Almost 150,000 computes has infected from the virus and there were 170,000 computers, which belong to finance ministry. The viruses' access thorough senior officials computers has canceled, but most of the infected computers used in the G20 Summit.

e. INDIA

In 2016, officials have reported a data breach to the Indian Banks. CISA Information Security audited the system and reported breach was a result of a malware injected into the payment gateway network of Hitachi Payment Systems. Approximately 3.2 million bankcards were seized. Many users reported card access without permission from locations of China. This caused a huge amount of card blocking and replacing situation in India.

Most of the countries have faced a cyber-attack while the technology is improving faster and faster. There can be given other examples such as a power cut cyber-attack to Ukraine.

VII. Rules and Regulations of Cyber Space

Several parties have attempted to come up with legal frameworks to clarify cyberspace or law of cyberspace and what is acceptable or not yet none of them broadly accepted.

a. Budapest Convention on Cybercrime

The Convention on Cybercrime is the first international agreement, which addresses internet and computer crime by using national laws and investigation techniques with compounding participation and cooperation between states in 2001. The Convention underlines criminal actions by using internet by discussing articles such as data interference, system interference, misuse of devices, computer-related forgery and fraud, offenses related to child pornography and infringements of copyright and related rights, attempt and aiding or abetting, and corporate liability. These subjects were examined under the chapters of measures to be taken at the national level and international co-operation.

Since it entered into force, important countries like Brazil and India refused to adopt the Convention and that they did not participate in its drafting. Russia opposes the Convention by stating adoption would violate.

b. The Tallinn Manual

Tallinn Manual is an academic and non-binding study. It all began with how international law, international humanitarian law especially jus ad bellum (authorization to start a war) apply to cyberspace, cyber warfare. The rules are restatements of international law in the cyber context. The Tallinn Manual prepared by the international groups of experts at the invitation of the NATO Cooperative Cyber Defense Centre of Excellence. They worked for the manual between 2009 and 2013 and published at 2013. Recently at February 2017 Tallinn Manual 2.0 was publish concerning fast-changing technology and cyberspace

In the foreword of the second manual, they explain the new version as "The scope of the 2013 manual was limited to international law on the use of force and international humanitarian law. In practice, many questions concerning the application of international law fall outside of its scope. Fortunately, situations of armed conflict are the exception rather than the rule. Most cyber activities take place in times of peace. The invitation that the NATO Cooperative Cyber

Defense Centre of Excellence extended to the experts to update the manual and explore the application of peacetime international law was, therefore, a welcome initiative. It offered a unique opportunity for exchanges and engagement between academic experts and national legal advisors."

VIII. Conferences, Meetings, and Organizations

Global Conference on Cyberspace (GCCS) was established to create internationally agreed rule perspective in cyberspace, and create a more focused and comprehensive communication between governments, civil society, and industry who uses internet on how to implement them.

The North Atlantic Treaty Organization (NATO) established Cooperative Cyber Defence (CCD) Center of Excellence (COE) in Estonia in 2017. They invited several experts to improve, re-create the Tallinn Manual 2.0.

The European Network and Information Security Agency (ENISA) was established in 2004 to strengthen the actions and the coordination to protect the privacy of information and prevent the cybercrime.

The United Nations Institute for Training and Research (UNITAR) has published a book, which called “Law of Cyber-Space - An Invitation to the Table of Negotiations”. This was an attempt to address the beginnings of an international agreement on the subject.

The International Criminal Police Organization (INTERPOL) has established numerous international organizations such as INTERPOL Working Parties on IT Crime, Training, and Operational Standards Initiative, National Central References Points Network, and the International Cybercrime Conference to fight against cyber warfare among its member countries.

IX. Questions to consider

Is it possible to limit cyberspace as? If it is how SPECPOL propose a solution?

How committee addresses to apply legal restrictions to cyber terrorism?

How committee takes action to prevent further cyber-attacks?

What other implementations can be applied in cyberspace?

By taking into consideration SPECPOL authorities, how could be the determination and punishment of the cyber-criminals?

Which international, regional, and global procedures can be taken to build a global stability in cyberspace?

How UN acts previous and how will they act respect to the cyber terrorism?

By taking into consideration that most of the States have a governmental unit and regulations or laws about cyberspace, how could it be possible to apply or harmonize these at international level?

X. References

http://www.umuc.edu/academic-programs/cyber-security/about.cfm

https://msu.edu/~plairsan/Makeover/History.htm

http://www.calmun.org/documents/GA4_17.pdf

https://gccs2017.in/about#goal

http://eds.a.ebscohost.com/eds/detail/detail?vid=0&sid=61ba3ecb-b67f-46c0-8b15-09c9f92658fb%40sessionmgr4007&bdata=JnNpdGU9ZWRzLWxpdmU%3d#AN=491171&db=nlebk

http://www.dictionary.com/browse/cyber?s=t

https://en.oxforddictionaries.com/definition/terrorism

https://en.oxforddictionaries.com/definition/cyberwarfare

http://www.investopedia.com/terms/c/cybersecurity.asp

https://techterms.com/definition/intranet

https://www.state.gov/documents/organization/229235.pdf page 10

https://www.linkedin.com/pulse/cyber-crime-v-cyber-terrorism-what-difference-matthew-kurnava/

https://www.rand.org/content/dam/rand/pubs/issue_papers/2005/IP245.pdf

https://www.checkmarx.com/2016/05/04/cyber-terrorism-real-threat-2/

http://resources.infosecinstitute.com/cyberterrorism-distinct-from-cybercrime/

https://academic.oup.com/cybersecurity/article/3/1/49/2999135

http://resources.infosecinstitute.com/cyberterrorism-distinct-from-cybercrime/

http://www.bbc.com/news/39655415

http://www.parismatch.com/Actu/Societe/Espionnage-a-Bercy-La-France-face-aux-pirates-146547

https://economictimes.indiatimes.com/industry/banking/finance/banking/security-breach-sbi-blocks-over-6-lakh-debit-cards/articleshow/54933861.cms

https://www.checkmarx.com/2016/05/04/cyber-terrorism-real-threat-2/

https://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF-E.pdf

http://foreignpolicy.com/2013/04/16/china-is-a-cyber-victim-too/